Period of a Discrete Cat Mapping

Freeman J. Dyson and Harold Falk

1. INTRODUCTION. In studying the dynamics of a mechanical system one uses time averages and phase-space averages [**1**] to describe the evolution. The existence and properties of the averages are part [**2**, **3**, **4**] of ergodic theory. The latter theory is not restricted to mechanical systems described by Newton's laws of motion, but also deals with abstract dynamical systems such as the abstract dynamical system involving the following mapping [**4**].

Let (x, y) denote a point in the unit square. The mapping takes (x, y) to the new point

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1. \tag{1.1}$$

The mapping preserves area (measure $d\mu = dx\,dy$); is associated with a discrete-time flow on a torus; and provides an example of a hyperbolic toral automorphism [**4**, **5**]. In an abstract sense the flow relates to the phase-space flow described by the Liouville Theorem [**6**].

Let $\vec{x}$ denote the initial point (x, y) and let $\vec{x}_n$ denote the image of $\vec{x}$ after n iterations of (1.1), $n = 0, 1, 2, \ldots$. The time average of a complex-valued function f, defined on the unit square and μ-integrable, is

$$\langle f(\vec{x}) \rangle_{\text{time}} = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\vec{x}_n), \tag{1.2}$$

and the phase-space average of f is

$$\langle f \rangle = \int_{\text{unit square}} f(\vec{x})\, d\mu \tag{1.3}$$

Since phase-space averages are widely employed and play a prominent role in statistical mechanics, a natural question is: Is $\langle f \rangle$ equal to $\langle f(\vec{x}) \rangle_{\text{time}}$? The following concept of mixing [**4**] has been a useful tool in pursuing an answer to that question.

Let $\mathscr{A}$ denote a measurable subset of $\mathscr{M}$ ($\mathscr{M}$ is the unit square in our example, and $\mu(\mathscr{M}) = 1$). Let $\mathscr{A}_n$ denote the image of $\mathscr{A}$ after n iterations of the mapping (1.1). If for every pair of measurable subsets $\mathscr{A}$ and $\mathscr{B}$ of $\mathscr{M}$,

$$\lim_{n \to \infty} \mu(\mathscr{A}_n \cap \mathscr{B}) = \mu(\mathscr{A})\mu(\mathscr{B})/\mu(\mathscr{M}), \tag{1.4}$$

the mapping (more precisely, the dynamical system) is mixing.

For a mixing dynamical system view $\mathscr{A}$ as a two-dimensional ink droplet and $\mu(\mathscr{A})/\mu(\mathscr{M})$ as the "concentration" of ink in the unit square. Then after "many" iterations the ratio $\mu(\mathscr{A}_n \cap \mathscr{B})/\mu(\mathscr{B})$ (for $\mu(\mathscr{B}) \neq 0$) represents the concentration of ink in $\mathscr{B}$. According to (1.4), that concentration should also be

$\mu(\mathscr{A})/\mu(\mathscr{M})$. Thus, the ink drop has been somewhat uniformly "smeared" over the unit square.

The mixing property is heuristically demonstrated [**4**, **2**] by placing a picture of a cat in the unit square and then displaying several subsequent images resulting from the flow. The images show that the cat tends to become "smeared" over the unit square.

It has been shown [**4**] that the above hyperbolic toral automorphism is mixing, and mixing implies [**4**] that

$$\langle f(\vec{x})\rangle_{\text{time}} = \langle f\rangle, \quad \text{almost everywhere.} \tag{1.5}$$

A mapping having the above mathematical properties and connections with statistical mechanics has an "intellectual domain of attraction," and we were drawn in. This paper documents our pleasant experience.

The computer is a convenient device for demonstrating mappings, where the screen serves as a two-dimensional lattice of points (pixels). For the purpose of demonstration, consider a square lattice of points and denote the points by (x, y). Restrict x and y to the integer values $0, 1, \ldots, N-1$ with the operations of addition and multiplication performed (mod N). The mapping (1.1) is approximated by the mapping

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \pmod N \tag{1.6}$$

where x and y are integers in $[0, 1, \ldots, N-1]$. N will typically be selected so as to make ample use of the capability of the screen; we take $N = 161$ as an example. Note that the computer deals precisely with the arithmetic operations of the mapping (1.6); the problem of round-off error does not arise.

Figure 1 displays "snapshots" of the early iterations of the mapping (1.6), starting with the initial "cat" configuration. The tendency to mix is evident, but one knows that the initial configuration must eventually return, since there are $2^{N\times N}$ possible configurations of the $N \times N$ pixels, where each pixel is either "on" or "off." However, for $N = 161$ the number $2^{N\times N}$ is large, and it was surprising to see the cat configuration return after only 24 iterations. This paper contains theorems which explain the observed periodicity.

It will be convenient to use the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{where } A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

and the Fibonacci sequence $u_0 = 0$, $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3, \ldots, [u_{n+2} = u_{n+1} + u_n]$. Then the nth iteration of the mapping (1.6) is

$$A^{2n} = \begin{pmatrix} u_{2n-1} & u_{2n} \\ u_{2n} & u_{2n+1} \end{pmatrix} \qquad (n = 1, 2, 3, \ldots). \tag{1.7}$$

For a given N the period m_N of the mapping (1.6) is the smallest positive integer n such that

$$\left.\begin{aligned} & u_{2n} \equiv 0 \pmod N \\ \text{and} \quad & \\ & u_{2n-1} \equiv 1 \pmod N. \end{aligned}\right\} \tag{1.8}$$

[Note that (1.8) implies $u_{2n+1} \equiv u_{2n+2} \equiv 1 \pmod N$.] Thus, the period is related to the divisibility properties of Fibonacci numbers.

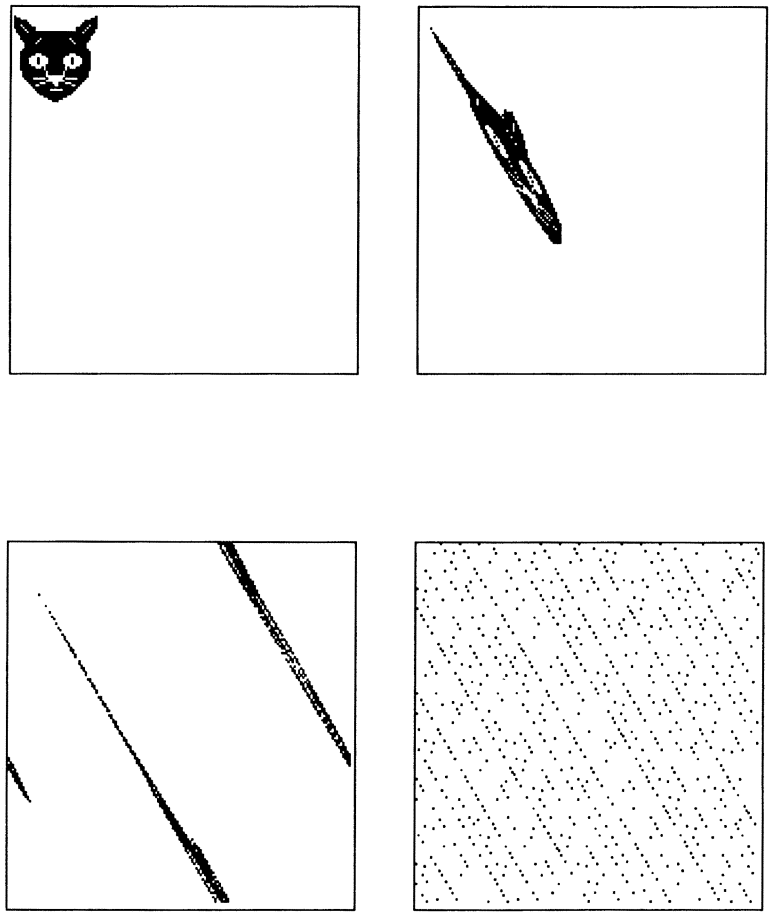

Figure 1. "Snapshots" of the initial "cat" configuration and of the images at $t = 1$, $t = 2$ and $t = 5$ under the mapping given by Eq. (1.6) for $N = 161$. That is, top row left to right: $t = 0$, $t = 1$; bottom row left to right: $t = 2$, $t = 5$.

We will use theorems contained in Hardy and Wright [**7**], and we refer to specific theorems as numbered in the fifth edition; e.g., HW Thm. 97 [**7**]. Two useful identities [**8**] are:

For any positive integers k, r

$$u_{k+r} = u_k u_{r+1} + u_{k-1} u_r \tag{1.9}$$

$$(-1)^k = u_{k+1} u_{k-1} - u_k^2. \tag{1.10}$$

These identities may be extended to all integer values k, r if one defines

$$u_{-k} = (-1)^{k-1} u_k \quad \text{for } k = 0, 1, 2, 3, \ldots . \tag{1.11}$$

2. UPPER BOUNDS FOR THE PERIOD. Our first upper bound for the period is $m_N \leq N^2/2$ for $N > 2$. Consequently, m_N does not grow exponentially with N.

To derive that bound we retrace the path of Vorob'ev [**9**] and write

$$u_n = \phi_n \pmod N \tag{2.1}$$

where ϕ_n is the least non-negative residue of u_n to modulus N. Consider the sequence of ordered pairs $\langle \phi_1, \phi_2 \rangle, \langle \phi_2, \phi_3 \rangle, \ldots, \langle \phi_n, \phi_{n+1} \rangle, \ldots$. There are at

most N^2 distinct pairs. Any set of $N^2 + 1$ pairs contains some equal ones among them.

Lemma 1 [9]. *The first pair that repeats in the above sequence is* $\langle 1, 1\rangle$.

Proof: Assume the opposite; i.e., that the first repeated pair is $\langle \phi_k, \phi_{k+1}\rangle$, where $k > 1$. Let us find in the sequence a pair $\langle \phi_r, \phi_{r+1}\rangle$ $(r > k)$ such that $\phi_k = \phi_r$, $\phi_{k+1} = \phi_{r+1}$. From the definition of the Fibonacci numbers

$$\phi_{r-1} = \phi_{r+1} - \phi_r \tag{2.2}$$

$$\phi_{k-1} = \phi_{k+1} - \phi_k \tag{2.3}$$

so

$$\phi_{r-1} = \phi_{k-1} \tag{2.4}$$

and we have

$$\langle \phi_{r-1}, \phi_r\rangle = \langle \phi_{k-1}, \phi_k\rangle. \tag{2.5}$$

But $\langle \phi_{k-1}, \phi_k\rangle$ is situated earlier in the sequence than $\langle \phi_k, \phi_{k+1}\rangle$; therefore $\langle \phi_k, \phi_{k+1}\rangle$ is not the first pair that repeats itself. So the supposition $k > 1$ is wrong, and we must have $k = 1$. That proves the Lemma.

Theorem 1 [9]. *For any positive integer N at least one number divisible by N can be found among the first* N^2 *Fibonacci numbers.*

Proof: From the Lemma $\langle 1, 1\rangle$ is the first pair that repeats itself. So $\langle \phi_t, \phi_{t+1}\rangle = \langle 1, 1\rangle$ for some integer t such that $1 < t \leq N^2 + 1$. Thus

$$\phi_t \equiv 1 \pmod{N} \tag{2.6}$$

and

$$\phi_{t+1} \equiv 1 \pmod{N}. \tag{2.7}$$

But

$$u_{t-1} = u_{t+1} - u_t; \tag{2.8}$$

therefore,

$$\phi_{t-1} \equiv 0 \pmod{N}, \tag{2.9}$$

and the Theorem is proved.

Lemma 2. *For* $N > 2$ *if* $u_n \equiv 0 \pmod{N}$ *and* $u_{n+1} \equiv 1 \pmod{N}$, *then n must be even.*

Proof: The Lemma is equivalent to the statement that for $N > 2$ if $A^n \equiv 1 \pmod{N}$, then n is even. But the determinant $\det(A) = -1$, so $\det(A^n) = (\det A)^n = (-1)^n \equiv 1 \pmod{N}$. Hence n must be even.

Theorem 2. *For* $N > 2$ *the period* m_N *of the mapping* (1.6) *satisfies*

$$m_N \leq N^2/2. \tag{2.10}$$

Proof: From Lemma 1 and Theorem 1, the first reappearance of the pattern 0, 1, 1 in the sequence $\phi_0, \phi_1, \phi_2, \phi_3, \ldots, \phi_n, \phi_{n+1}, \ldots$ occurs for $\phi_{t-1}, \phi_t, \phi_{t+1}$, where $0 < t - 1 \leq N^2$. From Lemma 2, $t - 1$ must be even. From the definition of the period one has $2m_N = t - 1$. That proves the Theorem.

Numerical results for m_N indicate that the bound is rather loose; nevertheless, the bound establishes that m_N does not grow exponentially with N. The method which will be used subsequently to prove Theorem 3 also gives a stronger Theorem than Theorem 1; viz.,

Theorem 1′. *For any positive integer N, at least one Fibonacci number $u_n \equiv 0 \pmod N$ with $n \leq 2N$.*

Remark. We have $n \leq 12N/7$ except in cases $N = 6 \cdot 5^\delta$, $\delta = 0, 1, 2, \ldots$, when $n = 2N$.

Remark. From Theorem 1′, for any positive integer N there is an $n \leq 2N$ such that $u_n \equiv 0 \pmod N$. Identity (1.9) then implies $u_{2n} \equiv 0 \pmod N$. One now may use Theorem 5 to write

$$m_N \leq 2n \leq 4N. \tag{2.11}$$

That is a substantial improvement over (2.10), but Theorem 3a is a little stronger still.

Next we give a much tighter upper bound for m_N. The bound, denoted by m^*, is always an integer multiple of the period m_N for the mapping (1.6). The bound is based on the following Theorem, which may be viewed as an extension of HW Thm. 180 [7].

Theorem 3. *Let p be a prime $\equiv \pm 1 \pmod{10}$. Then $A^{p-1} \equiv 1 \pmod p$. Let q be a prime $\equiv \pm 3 \pmod{10}$. Then $A^{q+1} \equiv -1 \pmod q$. For the prime 5, $A^{10} \equiv -1 \pmod 5$; and for the prime 2, $A^6 \equiv 1 \pmod 4$.*

Application of Theorem 3 to the periodicity of the mapping (1.6) is made as follows.

Consider a positive integer $N > 1$ and write N in terms of its prime factors p and q, which were referred to in the above Theorem.

$$N = \left(\prod_{p|N} p^\alpha\right)\left(\prod_{q|N} q^\beta\right)5^\gamma 2^\delta \tag{2.12}$$

where the notation $p|N$ means "p divides N." Since α will always be associated with p, and β with q, we will avoid the notation α_p and β_q.

As $A^{p-1} \equiv 1 \pmod p$, it follows from HW Thm. 78 [7] that $A^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$. Further, the congruence $A^{q+1} \equiv -1 \pmod q$ implies $A^{2(q+1)} \equiv 1 \pmod q$, and HW Thm. 78 [7] gives $A^{2(q+1)q^{\beta-1}} \equiv 1 \pmod{q^\beta}$. Finally, the congruence $A^{10} \equiv -1 \pmod 5$ implies $A^{2(10)5^{\gamma-1}} \equiv 1 \pmod{5^\gamma}$, and $A^6 \equiv 1 \pmod 4$ implies $A^{3\cdot 2^{\delta-1}} \equiv 1 \pmod{2^\delta}$.

For a given N, the period of the mapping (1.6) was defined to be the smallest positive integer m_N such that $A^{2m} \equiv 1 \pmod N$. To find an upper bound m^* on m_N, compute the least common multiple [LCM]

$$2m^* = LCM\left[(p-1)p^{\alpha-1}, 2(q+1)q^{\beta-1}, 2(10)5^{\gamma-1}, (3)2^\varepsilon\right] \tag{2.13}$$

with

$$\varepsilon = \text{Max}(\delta - 1, 1). \tag{2.14}$$

Each factor in (2.12) has a corresponding term in the LCM. Therefore (2.12) and

(2.13) imply

$$A^{2m^*} \equiv 1 \pmod{N}, \tag{2.15}$$

so that m^* is a multiple of m_N and

$$m_N \leq m^*. \tag{2.16}$$

In the particular case mentioned above, $N = 161 = 7 \cdot 23$; only the two primes $q = 7$ and $q = 23$ play a role, and $\beta = 1$ for each. Thus $m^* = 24$, equal to the value we found for m_N. Numerical results for m_N and m^* indicate that the inequality (2.16) is satisfied as an equality for most values of $N \leq 10^6$.

We call an integer N "primitive" if $m_N = m^*$. A primitive N is one whose period m_N achieves the upper bound, m^*. Thus, 161 is primitive. To our surprise we found that the great majority of small N are primitive. The first non-primitive N is 29, with $m_N = 7$, $m^* = 14$. We looked at three stretches of 100 values of N and found:

$$\begin{aligned} 1 \leq N \leq 100, &\qquad 96 \text{ are primitive,} \\ 901 \leq N \leq 1000, &\qquad 84 \text{ are primitive,} \\ 999901 \leq N \leq 1000000, &\qquad 82 \text{ are primitive.} \end{aligned}$$

So far as they go, these numbers suggest that the fraction of primitive N is tending to a limit substantially greater than 0.5 as $N \to \infty$. However, we conjecture that the opposite is true.

Conjecture. *The fraction of primitive integers not exceeding N has the asymptotic behavior*

$$F(N) \sim \frac{K}{\log\log\log N} \tag{2.17}$$

as $N \to \infty$, *where*

$$K = e^{-\gamma}\left(\frac{\log(10/3)}{\log 2}\right) = 0.975, \tag{2.18}$$

and γ *is Euler's constant.*

Since $\log\log\log 10^6 = 0.965$, our numerical data do not begin to test the validity of (2.17).

The argument leading to (2.17) is probabilistic and makes no claim to be rigorous. According to HW Thm. 436 [7], almost all integers not exceeding N have about

$$y = \log\log N \tag{2.19}$$

distinct prime factors, which will appear in the definition (2.13) of m^*. For N to be primitive it is necessary and sufficient that

$$A^{2m^*/s} \not\equiv 1 \pmod{N}, \tag{2.20}$$

for every prime s dividing $2m^*$. Now the matrix

$$B = A^{2m^*/s} \tag{2.21}$$

satisfies the congruence

$$B^s \equiv 1 \pmod{N}. \tag{2.22}$$

We wish to estimate the probability that $B \not\equiv 1 \pmod{N}$. If N is a p-prime, then s must be a divisor of $(N-1)$ and the congruence (2.22) has exactly s roots. We assume that each of the roots has equal probability s^{-1} of being (2.21). Then the probability that (2.20) holds is

$$1 - s^{-1}. \tag{2.23}$$

If N is a q-prime, then s must be a divisor of $2(q+1)$ and again the congruence (2.22) has s roots in the field generated by $A \pmod{N}$. If s is an odd prime, the estimate (2.23) holds as before. But for $s = 2$, we know from Theorem 3 that $B \equiv -1 \pmod{N}$ and therefore (2.20) holds with probability 1.

When N is composite, we assume that the probabilities for (2.20) to hold are independent for all primes s dividing $2m^*$. The probability for N to be primitive is then

$$F(N) = \left(1 - \tfrac{1}{2}(1-Q)\right) \prod_{s>2} \left(1 - s^{-1} d_s\right), \tag{2.24}$$

where d_s is the probability that the odd prime s divides $2m^*$, and Q is the probability that the highest power of 2 in the LCM (2.13) belongs to one of the terms $2(q+1)$. Since each s has roughly y chances to divide one of the factors appearing in (2.13),

$$d_s = 1 - (1 - s^{-1})^y. \tag{2.25}$$

To estimate Q, we suppose that each term $(p-1)$ or $(q+1)$ appearing in (2.13) is divisible by 2^k with probability 2^{-k}, $k = 1, 2, 3, \ldots,$. For large N, the number of p-primes and q-primes will both be approximately

$$M = \tfrac{1}{2} y. \tag{2.26}$$

The probability that k_1 is the highest power of 2 dividing any $(p-1)$ is $r(k_1)$, and the probability that k_2 is the highest power of 2 dividing any $(q+1)$ is $r(k_2)$, where

$$r(k) = (1 - 2^{-k})^M - (1 - 2^{1-k})^M. \tag{2.27}$$

Q is the probability that

$$1 + k_2 \geq k_1. \tag{2.28}$$

Thus

$$\begin{aligned} Q &= \sum\sum_{1+k_2 \geq k_1} r(k_2) r(k_1) \\ &= \sum_k \left((1 - 2^{-k})^M - (1 - 2^{1-k})^M\right)(1 - 2^{-1-k})^M. \end{aligned} \tag{2.29}$$

For large M we may replace the sum over k by an integral over a continuous variable u given by

$$e^{-u} = 1 - 2^{-k}. \tag{2.30}$$

Then (2.29) becomes in the large-M limit

$$\begin{aligned} Q &= (\log 2)^{-1} \int_0^\infty (e^u - 1)^{-1} (e^{-(3/2)Mu} - e^{-(5/2)Mu})\, du \\ &= \left(\log \tfrac{5}{3} / \log 2\right), \end{aligned} \tag{2.31}$$

and (2.24) becomes

$$F(N) = \left(\log \frac{10}{3} \Big/ \log 2\right) \prod_s (1 - s^{-1} d_s), \tag{2.32}$$

with the product extending over all primes s. A more exact analysis of the sum (2.29) shows that Q contains also an extravagantly small oscillating term

$$\sum_{k=1}^{\infty} A_k \cos\left(2\pi k (\log 2)^{-1} (\log\log\log N) + \delta_k\right), \tag{2.33}$$

with amplitude

$$A_k \sim \exp\left(-\pi^2 (\log 2)^{-1} k\right) \sim 10^{-6k} \tag{2.34}$$

which we shall neglect.

We return to (2.32) with d_s given by (2.25). The factors in the product can be crudely approximated by

$$\begin{aligned} d_s &= (1 - s^{-1}) \quad \text{for } s \le y, \\ d_s &= 1 \qquad\quad\ \ \text{for } s > y. \end{aligned} \tag{2.35}$$

The error in (2.35) is small when s is either small or large compared with y. The maximum error is of order y^{-1} for primes s in the neighborhood of y. The number of such primes is of order

$$(y/(\log y)). \tag{2.36}$$

Therefore, the fractional error introduced by (2.35) into the product (2.32) is of order $(\log y)^{-1}$. A more careful analysis shows that the leading term in the error is a factor

$$1 - \gamma (\log y)^{-1}, \tag{2.37}$$

where γ is Euler's constant. Neglecting this factor, we find from (2.32) and (2.35)

$$F(N) \sim \left(\log \tfrac{10}{3} / \log 2\right) \prod_{s \le y} (1 - s^{-1}). \tag{2.38}$$

Finally, HW Thm. 430 [7] (Mertens's Theorem) says

$$\prod_{s \le y} (1 - s^{-1}) \sim \frac{e^{-\gamma}}{\log y}, \tag{2.39}$$

and this with (2.18), (2.19), and (2.38) gives (2.17).

From (2.13) and (2.16) one may derive a simpler upper bound for m_N.

Theorem 3a.

$$m_N \le 3N. \tag{2.40}$$

Moreover, (2.40) *holds with equality if and only if*

$$N = 2 \cdot 5^{\gamma}. \tag{2.41}$$

For all N except for (2.41) *we have*

$$m_N \le 2N, \tag{2.42}$$

with equality only for

$$N = 5^{\gamma}, \qquad N = 6 \cdot 5^{\gamma}. \tag{2.43}$$

For all N except for (2.41) *and* (2.43) *we have*

$$m_N \le \frac{12}{7} N. \tag{2.44}$$

We could find smaller bounds with larger lists of exceptions, but beyond (2.44) it seems unprofitable to go.

Proof of (2.40)–(2.44). Consider the ratio

$$R = (m^*/N) \geq (m_N/N), \tag{2.45}$$

with N given by (2.12) and m^* by (2.13). The definition of an LCM gives

$$2R \leq \left(\prod_{p|N}(1 - p^{-1})\right)\left(\prod_{q|N}\left[2(1 + q^{-1})\right]\right) \cdot 4 \cdot 3 \cdot 2^{-k} \tag{2.46}$$

where the factor 4 appears if $\gamma \geq 1$, the factor 3 appears if $\delta \geq 1$, and k is the number of powers of 2 that appear redundantly in the various terms of (2.13). We wish to choose N to make R as large as possible. By (2.46), R will be increased by dropping all the p-primes from N. Since each q-prime gives a term in (2.13) divisible by 4, R will be increased by dropping all of the q-primes except one, and by dropping all except one power of 2. We are left with only the following simple choices for N giving possibly maximum values for R,

$$N = 5^\gamma, 5^\gamma \cdot 3^\beta, 5^\gamma \cdot 7^\beta, 2 \cdot 5^\gamma, 6 \cdot 5^\gamma, 2 \cdot 5^\gamma \cdot 7^\beta, \tag{2.47}$$

giving respectively

$$R = 2, 4/3, 8/7, 3, 2, 12/7. \tag{2.48}$$

This proves the inequalities (2.40), (2.42), (2.44) and proves that the cases of equality are at most (2.41) and (2.43). It remains to prove that equality holds, i.e., $m_N = m^*$, in the cases (2.41), (2.43).

The Lucas numbers v_k are related to the Fibonacci numbers by

$$v_k = u_{k-1} + u_{k+1}. \tag{2.49}$$

By (1.7) and (1.11), the matrix A generates Fibonacci and Lucas numbers by

$$A^{2k} + A^{-2k} = v_{2k} \tag{2.50}$$

$$A^{2k} - A^{-2k} = u_{2k} \cdot \sqrt{5}, \tag{2.51}$$

where $\sqrt{5}$ [in this section] stands for the matrix

$$\sqrt{5} = A + A^{-1} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}, \tag{2.52}$$

whose square is 5. Now (2.50) and (2.51) give

$$v_{4k} = 5 \cdot u_{2k}^2 + 2, \tag{2.53}$$

$$u_{10k} = u_{2k}(1 + v_{4k} + v_{8k}) = 5 \cdot u_{2k}(1 + u_{2k}^2 + u_{4k}^2). \tag{2.54}$$

(2.54) implies

$$u_{10k} \equiv 0 \pmod 5, \tag{2.55}$$

$$u_{50k}/u_{10k} \equiv 5 \pmod{125}. \tag{2.56}$$

Thus u_{50k} is divisible by exactly one more power of 5 than u_{10k}. Now Theorem 3 with (2.51) shows that u_{2k} is periodic (mod 5) with period 10, so that

$$u_{2k} \not\equiv 0 \pmod 5 \quad \text{for } k \not\equiv 0 \pmod 5. \tag{2.57}$$

This with (2.54) implies

$$u_{10k} \not\equiv 0 \pmod{25} \quad \text{for } k \not\equiv 0 \pmod 5. \tag{2.58}$$

Together (2.55), (2.56), (2.57), and (2.58) imply

$$u_{2k} \equiv 0 \pmod{5^\gamma} \quad \text{if and only if } k \equiv 0 \pmod{5^\gamma}. \tag{2.59}$$

This means that for any N divisible by 5^γ, m_N is also divisible by 5^γ.

Consider in particular $N = 2 \cdot 5^\gamma$, which has m_N dividing $m^* = 6 \cdot 5^\gamma$. We have proved that m_N is divisible by 5^γ. Since N is divisible by 5 and by Theorem 3

$$A^{10} \equiv -1 \pmod{5}, \tag{2.60}$$

m_N must also be divisible by 2. Since N is even, m_N must be divisible by 3. Therefore $m_N = m^*$ and (2.40) holds with equality. The same argument shows that (2.42) holds with equality for N given by (2.43).

3. LOWER BOUNDS FOR THE PERIOD AND EXPLICIT VALUES FOR PARTICULAR CASES.

Theorem 4. *Both* $u_{4n} \equiv 0 \pmod{N}$ *and* $u_{4n-1} \equiv 1 \pmod{N}$ *if and only if*

$$u_{2n} \equiv 0 \pmod{N}. \tag{3.1}$$

Proof: The identities

$$u_{4n} = u_{2n} v_{2n}, \tag{3.2}$$

$$u_{4n-1} - 1 = u_{2n} v_{2n-1}, \tag{3.3}$$

imply the "if" part of the theorem immediately. The "only if" is equivalent to the statement that (v_{2n-1}, v_{2n}) are coprime, which is contained in HW Thm. 179 [7].

Theorem 5. *For* $N \geq 2$ *let* n *be the smallest positive integer such that* $u_{2n} \equiv 0$ *(mod* N*). Then either* $m_N = n$ *or* $m_N = 2n$.

Proof: By Theorem 4, n is the smallest integer such that

$$A^{4n} \equiv 1 \pmod{N}, \tag{3.4}$$

while m_N is the smallest such that

$$A^{2m_N} \equiv 1 \pmod{N}. \tag{3.5}$$

Integers satisfying (3.4) are multiples of n, and integers satisfying (3.5) are multiples of m_N. Therefore, m_N is a multiple of n, and $2n$ is a multiple of m_N. The conclusion follows.

Theorem 6. *Given* $N = u_{2n}$ *with* $n = 2, 3, \ldots$; *there does not exist an* $N' > N$ *with even period,* $m_{N'} \leq 2n$.

We give the proof of Theorem 7; the proof of Theorem 6 is similar.

Theorem 7. *Given* $N = v_{2n-1}$ *with* $n = 2, 3, \ldots$; *there does not exist an* $N' > N$ *with odd period,* $m_{N'} \leq 2n - 1$.

Proof: Assume $m_{N'} = 2n' - 1 \leq 2n - 1$ so that

$$u_{4n'-2} \equiv 0 \pmod{N'} \tag{3.6}$$

and

$$u_{4n'-3} \equiv 1 \pmod{N'}. \tag{3.7}$$

Then from Theorem 4

$$u_{2n'-1} \equiv 0 \pmod{N'}. \tag{3.8}$$

But if $2n' - 1 \leq 2n - 1$, then

$$\begin{aligned} u_{2n'-1} &\leq u_{2n-1} < u_{2n-1} + 2u_{2n-2} \\ &= u_{2n} + u_{2n-2} \\ &= N < N'. \end{aligned} \tag{3.9}$$

That contradicts (3.8) and completes the proof of the Theorem.

Corollary. *For $N' > v_{2n-1}$ with $n = 2, 3, \ldots$; $m_{N'} > 2n$.*

Proof: Since $u_{2n} + u_{2n-2} > u_{2n}$, the condition $N' > u_{2n} + u_{2n-2}$ implies the condition $N' > u_{2n}$. By Theorem 6 there are no even periods $m_{N'} \leq 2n$, and by Theorem 7 there are no odd periods $m_{N'} \leq 2n - 1$. That proves the corollary.

The corollary provides a "staircase" lower bound for m_N as a function of N. This bound may be expressed in the following way.

Define

$$\begin{aligned} N(n) &= u_n \quad \text{for } n \text{ even} \\ &= v_n \quad \text{for } n \text{ odd} \end{aligned} \tag{3.10}$$

and let

$$\lambda_+ = (1 + \sqrt{5})/2. \tag{3.11}$$

Then for n even and $N > N(n)$, any even period

$$m_N > n > \left[\log\left(N(n)\sqrt{5}\right)\right]/\log \lambda_+ \tag{3.12}$$

and for n odd and $N > N(n)$, any odd period

$$m_N > n > [\log N(n)]/\log \lambda_+. \tag{3.13}$$

These results may be summarized in

Theorem 8. *For any integer N,*

$$m_N > \left[\log\left(N\sqrt{5}\right)\right]/\log \lambda_+ \quad \text{if } m_N \text{ is even}, \tag{3.14}$$

$$m_N > [\log N/\log \lambda_+] \quad \text{if } m_N \text{ is odd}. \tag{3.15}$$

In the context of chaos, others [**10**] have displayed an approximate recurrence of a digitized image of an appropriately selected subject; viz., Henri Poincaré. The importance of background fluctuations is pointed out in that article.

Theorem 9.

(a) *For $N = u_{2n}$,* $m_N = 2n, (n > 1)$. (3.16)
(b) *For $N = u_{2n-1}$,* $m_N = 4n - 2, (n > 2)$. (3.17)
(c) *For $N = v_{2n}$,* $m_N = 4n$. (3.18)
(d) *For $N = v_{2n-1}$,* $m_N = 2n - 1$. (3.19)
(e) *For $N = v_{2n} - 1$,* $m_N = 6n$. (3.20)
(f) *For $N = v_{2n} + 1$,* $m_N = 3n$. (3.21)

[Note, e.g., $N = 842, 843, 844$ yield $m_N = 42, 28, 21$, respectively.]

Proof: The proofs of each part are similar so we choose to select a few for detailed presentation and sketch the others. For part (a) since $u_{2n} \equiv 0 \pmod{N}$, we find from Theorem 4 that $2n$ satisfies the conditions defining m_N and is therefore a multiple of m_N. But $u_{2m_N-1} \equiv 1 \pmod{N}$ implies $u_{2m_N-1} > u_{2n}$ and $2m_N - 1 > 2n$. Therefore, $2n$ can only be m_N.

Part (c) is proved by using $u_{4n} = u_{2n}v_{2n} \equiv 0 \pmod{N}$ and Theorem 4 to establish that $4n$ is a multiple of m_N. From the Corollary following Theorem 7 one concludes that $m_N > 2n$. Consequently, $4n = m_N$.

Part (d) is proved by making use of the two identities $u_{4n-2} = u_{2n-1}v_{2n-1}$ and $u_{4n-1} - 1 = u_{2n}v_{2n-1}$ to show that $2n - 1$ is a multiple of m_N. But $u_{2m_N-1} \equiv 1 \pmod{N}$ implies $u_{2m_N-1} > N$, where $N = v_{2n-1} > u_{2n-1}$ so that $2n - 1 < 2m_N$. A multiple of m_N satisfying the latter condition can only be m_N itself. Parts (e) and (f) are proved by using the identity $u_{6n} = u_{2n}(v_{2n} - 1)(v_{2n} + 1)$ along with part (a). The proof of part (b) is a bit more involved. One uses (1.9) to obtain $u_{4n-2} \equiv 0 \pmod{N}$ and then one uses Theorem 4 to obtain $A^{8n-4} \equiv 1 \pmod{N}$ so m_N divides $4n - 2$. But $N > v_{2n-3}$, so the Corollary following Theorem 7 says $m_N > 2n - 2$. The only possibilities are $m_N = 4n - 2$ or $2n - 1$. Assume that $m_N = 2n - 1$. Then $u_{4n-3} \equiv 1 \pmod{u_{2n-1}}$, but $u_{4n-3} = 1 + u_{2n-2}v_{2n-1}$ so $u_{2n-2}v_{2n-1} \equiv 0 \pmod{u_{2n-1}}$. According to HW Thm. 179 [7], u_k and u_{k+1} are coprime, while u_k and v_k have at most one common factor 2. Thus, the congruence $u_{2n-2}v_{2n-1} \equiv 0 \pmod{u_{2n-1}}$ is possible only if $u_{2n-1} = 1$ or 2, $n = 1$ or 2. This explains why (b) fails for $n \leq 2$.

REFERENCES

1. R. Z. Sagdeev, D. A. Usikov and G. M. Zaslavsky, *Nonlinear Physics*, Harwood, New York, 1988.
2. A. S. Wightman in *Statistical Mechanics at the Turn of the Decade*, edited by E. G. D. Cohen, Marcel Dekker, New York, 1971.
3. I. E. Farquhar in *Irreversibility in the Many-Body Problem*, edited by J. Biel and J. Rae, Plenum, New York, 1972.
4. V. I. Arnold and A. Avez, *Ergodic Problems in Classical Mechanics*, Addison-Wesley, Reading, Massachusetts, 1989.
5. J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*, Springer-Verlag, New York, 1986.
6. V. I. Arnold, *Ordinary Differential Equations*, MIT Press, Cambridge, Massachusetts, 1978.
7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press, Oxford, England, 1988.
8. R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, Massachusetts, 1989; equations 6.103 and 6.108.
9. N. N. Vorob'ev, *Fibonacci Numbers*, Blaisdell, New York, 1961.
10. J. P. Crutchfield, J. D. Farmer, N. H. Packard, R. S. Shaw, *Scientific American*, 255 (December 1986) 46–57.

The Institute for Advanced Study
Princeton, NJ 08540

Department of Physics
City College, CUNY
New York, NY 10031